# Information Security Standard

This Information Security Standard sets forth Elanco Animal Health's ("Elanco") information security requirements for Suppliers with respect to the confidentiality, integrity and availability of Information (defined below). Any additional Supplier obligations related to Information security under any agreement with Elanco are in addition to the requirements of this Information Security Standard.

As used herein, "Information" encompasses both Company Information and Personal Information that we use for business purposes (hereinafter independently and/or collectively referred to herein as "Information").
Personal Information means any information as defined in Elanco's Supplier Privacy Standard.
Company Information means any confidential or proprietary information as defined as such (or with a similar designation) in any written agreement between Supplier and Elanco.

As used herein, "Supplier Information System" means an information system that is owned or operated by a Supplier or Supplier's subcontractor(s) that handles Elanco Information by: (i) creating; (ii) editing; (iii) managing; (iv) processing; (v) accessing; (vi) receiving; (vii) transferring; (viii) destroying; (ix) storing; or (x) hosting, in any format, including, but not limited to: (a) systems; (b) cloud environments; (c ) production and non-production environments; (d) electronic assets and devices (including company-provided and "bring your own device"); and (e )hard copy versions.

Supplier shall handle the confidentiality, integrity and availability of Elanco's Information by utilizing the following minimum safeguarding requirements, controls, and procedures ("Minimum Safeguards"):

1. Limit handling of Elanco Information in Supplier Information System access to authorized users, processes acting on behalf of authorized users, or authorized devices (including other information systems):
   a. Identify Supplier Information System users, processes acting on behalf of authorized users, and authorized devices.
   b. Authenticate the identities of users, processes, and devices as a prerequisite to allowing access to Supplier Information Systems.
   c. Limit Supplier Information System access to trained, authorized users that have a business need to know to perform job duties, with password strength requirements that meet common security standards (e.g. ISO, NIST).

2. Limit physical access to Supplier Information Systems, equipment, and the respective operating environments:
   a. Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
   b. Data centers must be under physical control, with access formally managed based on business need.
   c. Data Centers must have environmental controls (temperature, humidity, power backup).

3. Monitor, control, and protect Information at the external boundaries and key internal boundaries of the Supplier Information Systems, including:
   a. Hardening for operating systems, applications, and network devices (e.g. Defense in Depth), such as intrusion detection, anti-virus and anti-malware.

b. Patching for operating system and major component updates upon security related patch release and evaluation in accordance with common security standards (e.g. ISO, NIST).
c. Logging activities documented and performed in accordance with common security standards (e.g., ISO, NIST).
d. Enabling encryption for data in transit with encryption procedures and practices that meet common security standards (e.g. ISO, NIST).
e. Permitting storage or transferring of Information using removable storage devices only through a documented process.
f. Performing periodic scans of Supplier Information Systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
g. Regularly backing up applicable systems and data. Backups must be appropriately secured from loss, damage, and unauthorized access and be periodically tested for viability.
h. Documenting privileged administrative user accounts as different than a standard user account, having unique user login ID's

4. Supplier shall notify Elanco within 72 hours of suspected or known security incidents that have potential impact to Information.

5. Supplier shall retain Information only for as long as specified within the applicable agreement, except to the extent that a longer retention period is required by applicable law or regulations. At the conclusion of the engagement, the Supplier must return, delete or securely destroy Information as instructed by Elanco, using asset disposal controls that meet common security standards (e.g. ISO, NIST).

6. At minimum, Supplier shall require compliance to these Minimum Safeguards by all its subcontractors that handle Elanco Information that resides outside Elanco's environment and/or when the Supplier has remote access connection to Elanco's environment.

7. These requirements will be applicable only for Suppliers building/supplying systems, software or applications for Elanco:
   a. A defined Systems Development Engineering Methodology, aligned to industry standards, must be formally implemented with policies, procedures and standards communicated and followed.
   b. A defined change/release management policy/procedure for planned software changes and bug fixes must be formally implemented.